

# Leading with Identity: Azure Active Directory

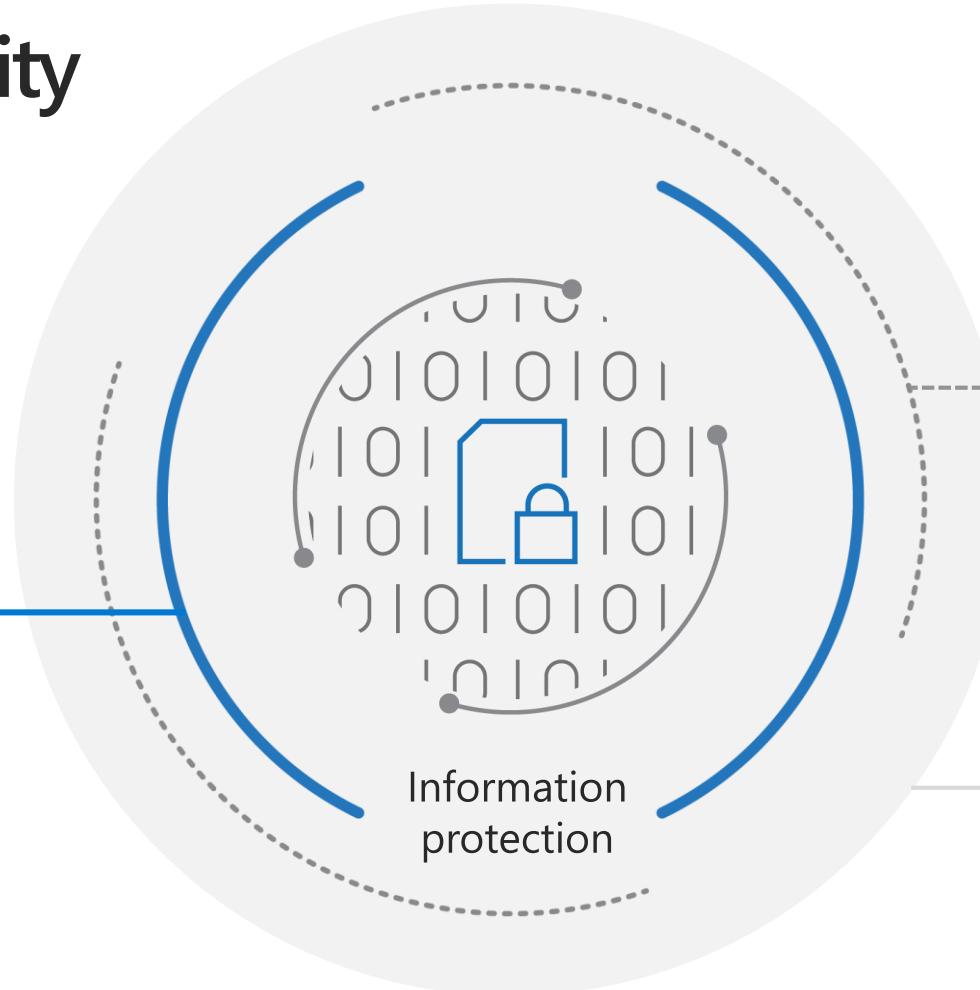
Joe Losinski  
Partner Technology Strategist



# Microsoft 365 Security



Identity & access management



Data is your most important company asset

Security starts with great user authentication

Correlate threat information and automatically respond

Optimize with security insights and configuration tools



Threat protection

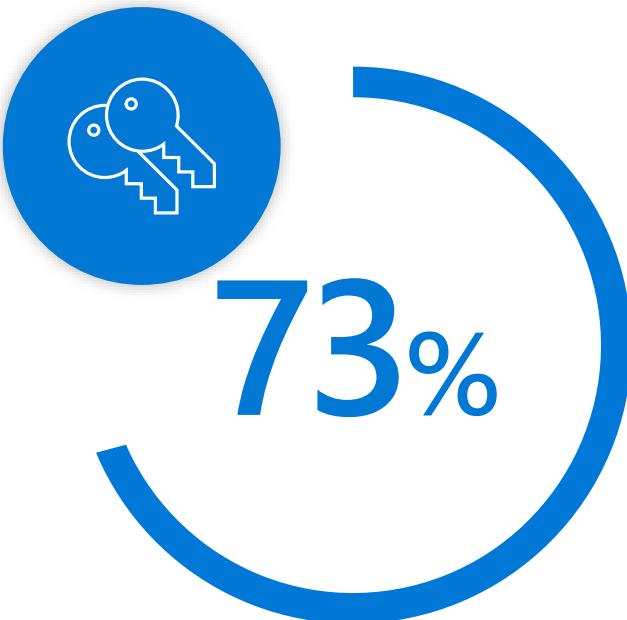


Security management

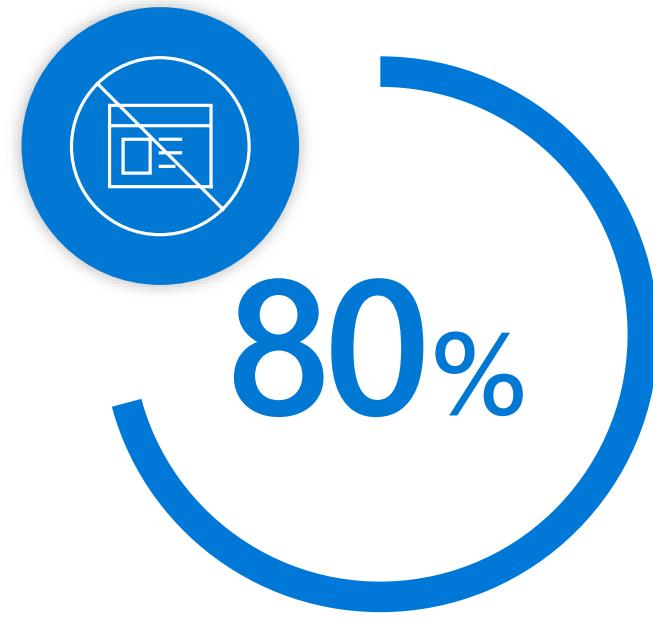
# User credentials are constantly at risk of a breach



of breaches are caused  
by credential theft

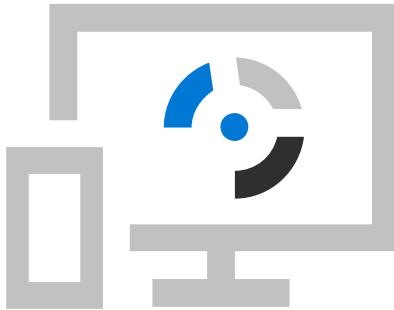


of passwords  
are duplicates



of employees use non-  
approved apps for work

# Identity challenges for today's organizations



Explosion of apps, devices, and users outside of the corporate network



Increase in identity attacks and lack of visibility and control

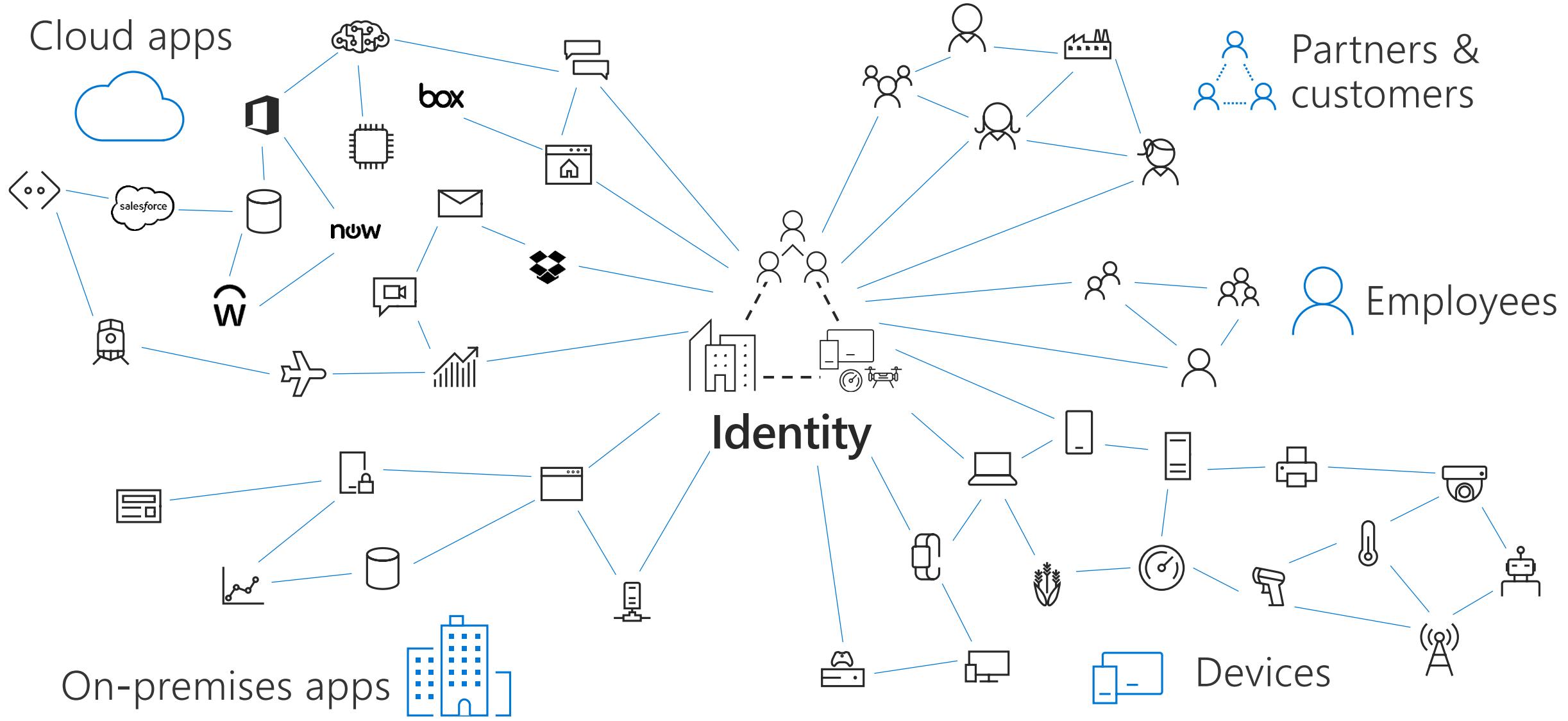


Evolving data privacy and security regulations to comply with



Demands for increased productivity and IT modernization

# Identity is the new control plane



# Microsoft Azure Active Directory

Your universal platform for managing and securing identities



## MODERNIZE ACCESS

[Connect your users to any app](#)

Single Sign-On  
Azure AD Connect  
Automated User Lifecycle  
Self-Service for End Users  
Access from Anywhere

## SECURE & GOVERN

[Safeguard user credentials](#)

Strong Authentication  
Conditional Access  
Identity Protection  
Privileged Identity Mgmt  
Identity Governance

## CONNECT & COLLABORATE

[Interact with customers and partners](#)

Customer & Partner Identity and Access Management  
Cross-Tenant Collaboration  
Personalized Customer Journeys  
Connect with Any User

## DEVELOP & INTEGRATE

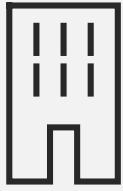
[Accelerate adoption of your apps](#)

Open standards-based Identity platform  
App Integration  
Microsoft Graph  
Identity for IaaS

# Why Microsoft

# The world's #1 enterprise identity service

**19.3M**  
organizations



**1.2B**  
identities



**810K**  
Third-party apps  
in Azure AD



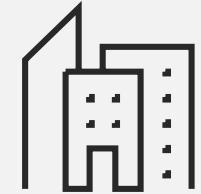
**100M**  
paid Azure AD/EMS  
seats



**8B**  
daily Azure AD  
authentications



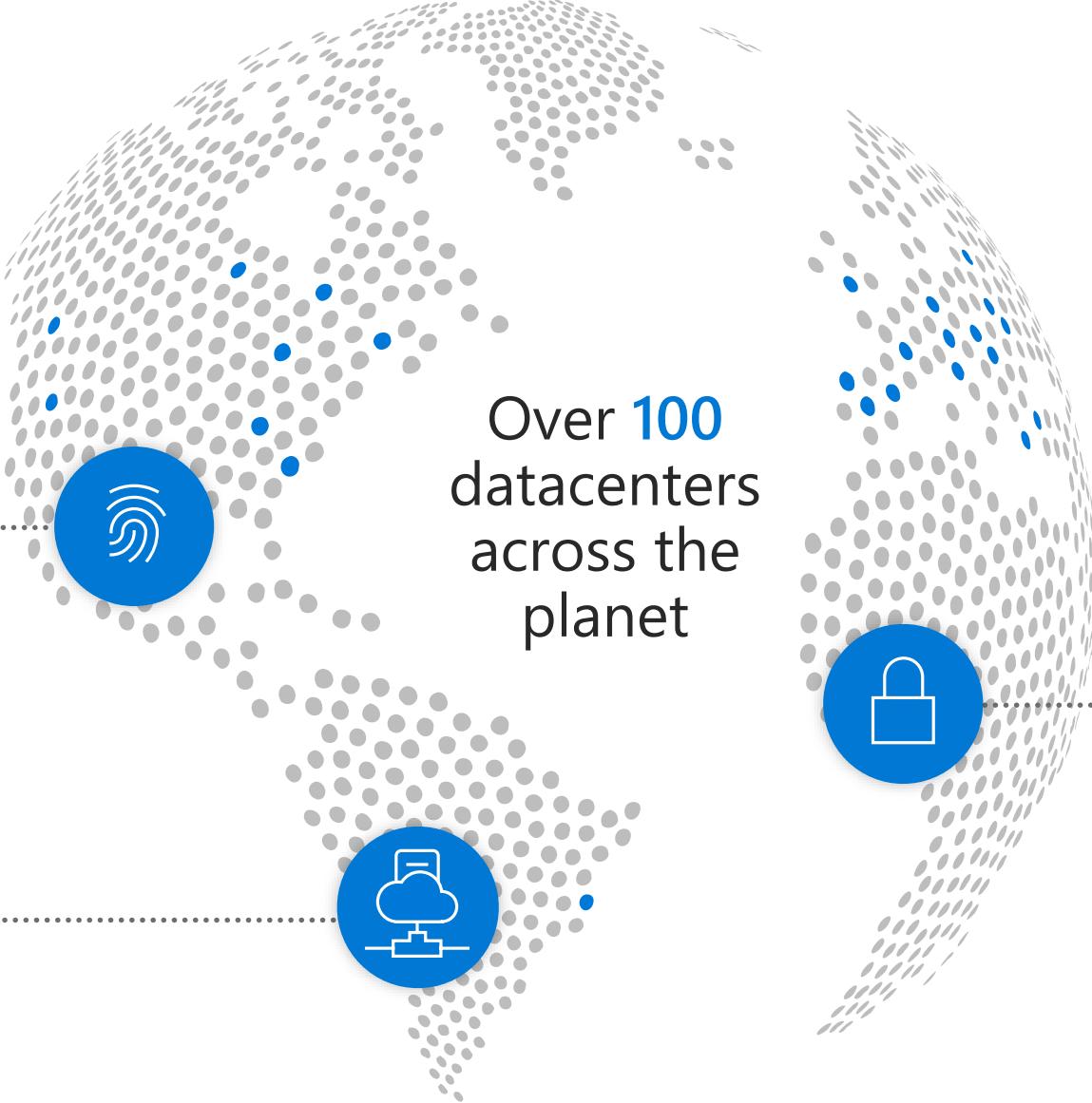
**90%**  
of Fortune 500  
companies



Jan 2019

# The most trusted platform

Each **physical datacenter** protected with world-class, multi-layered protection



Over **100** datacenters across the planet

**Global cloud infrastructure** with secure hardware and data segregation

Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- 3500+ global security experts

# The most compliant platform



More certifications than any other cloud provider



Industry leader for customer advocacy and privacy protection



Unique data residency guarantees

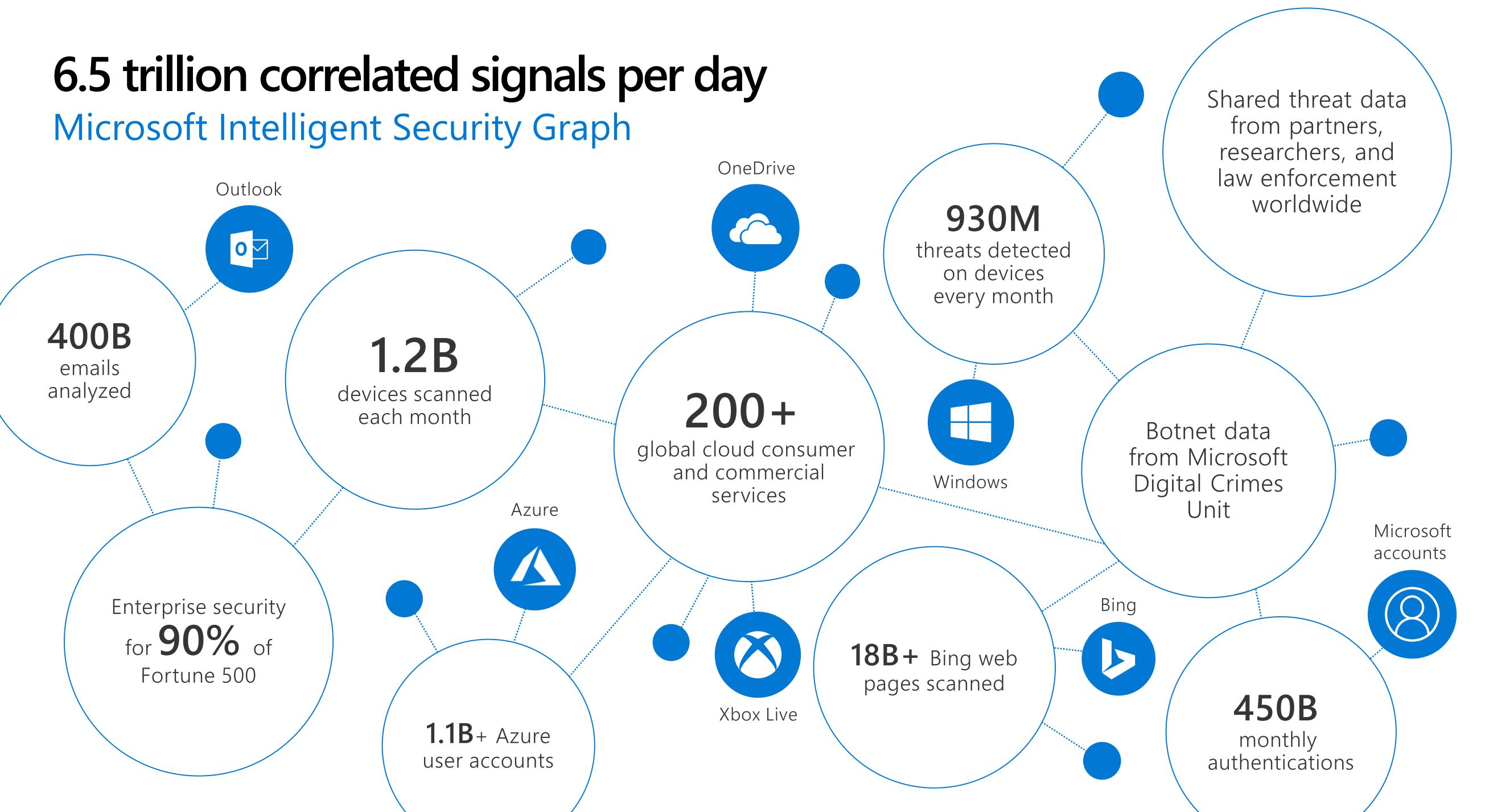


Microsoft is committed to GDPR compliance



# 6.5 trillion correlated signals per day

## Microsoft Intelligent Security Graph



# Microsoft is a leader in Access Management for Vision & Execution



At Microsoft, we focus on both vision and execution of our strategy to help you where you are at today and for the identity needs of tomorrow.

## Source: Gartner, Inc., Magic Quadrant for Access Management

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

# Azure Active Directory

## Modernize Access



MODERNIZE ACCESS

# Start with an identity foundation from the cloud



Seamless access to apps



Automated provisioning



Empower self-service

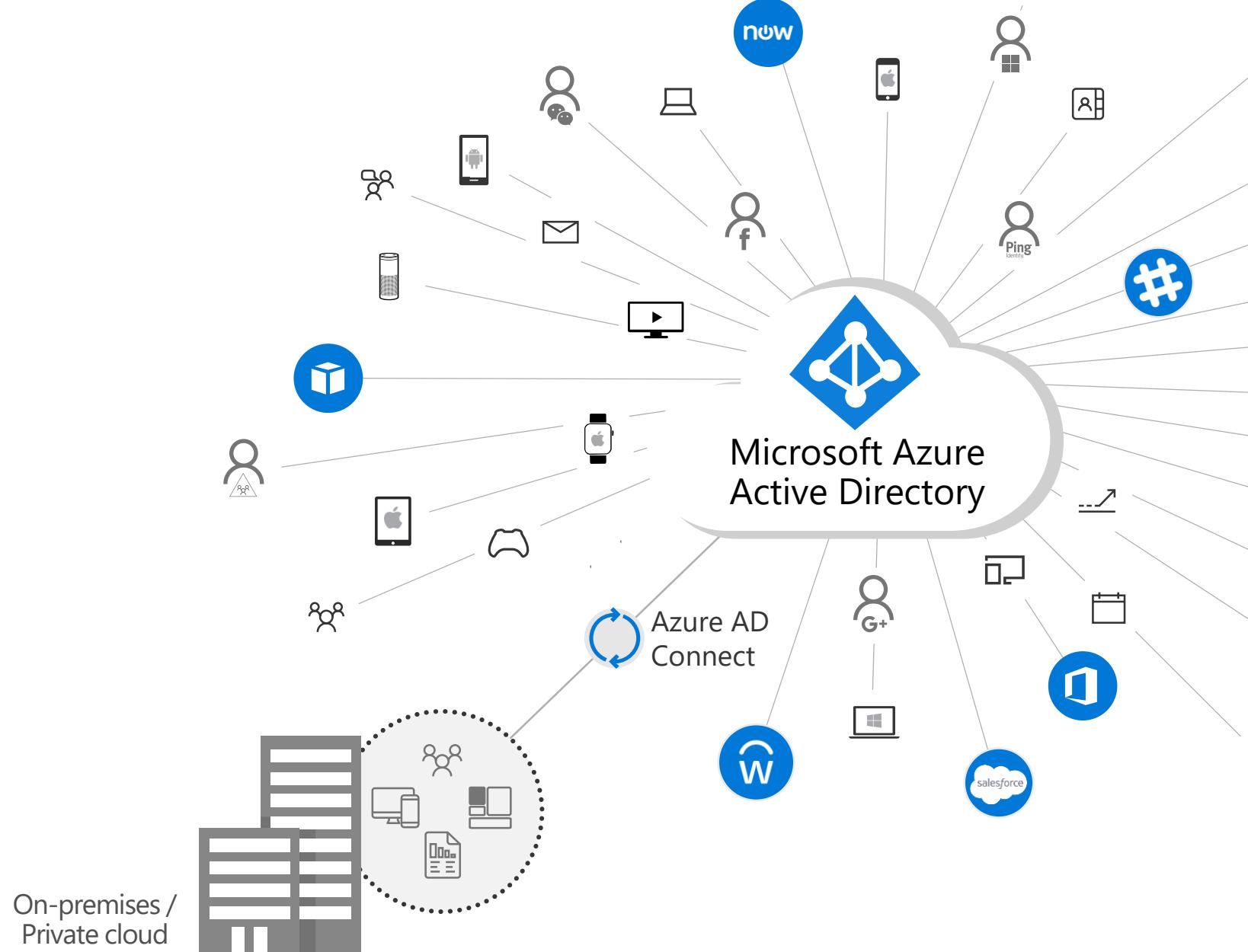
**Right for the modern workplace, right for the hybrid world.**



## MODERNIZE ACCESS

# Seamless access to apps

- One common identity for single sign-on
- Connect users to ALL the apps they need
- Access on-premises apps without using a VPN





MODERNIZE ACCESS

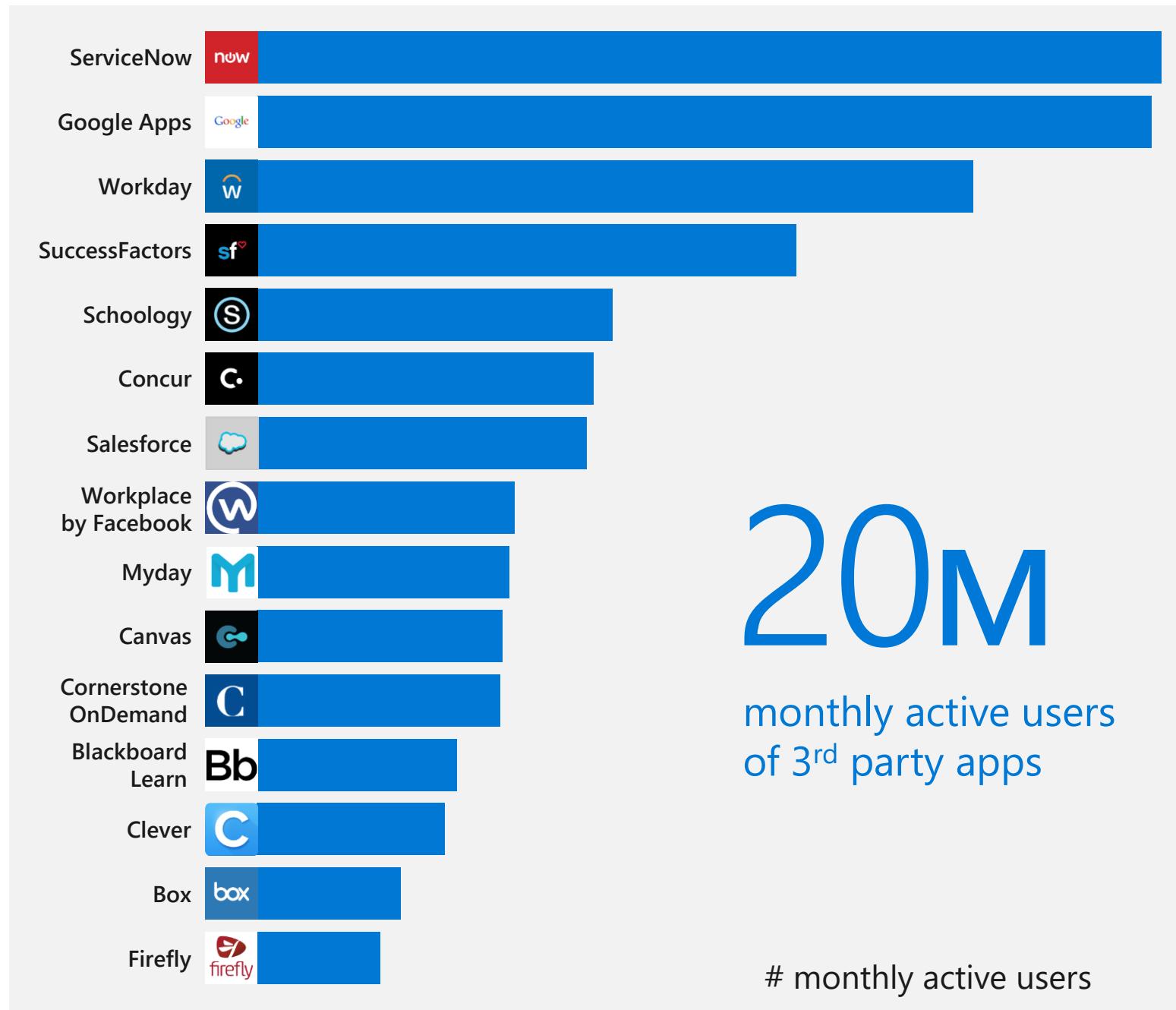
# Azure Active Directory

## 3<sup>rd</sup> party applications

810,000

active apps integrated with  
Azure Active Directory

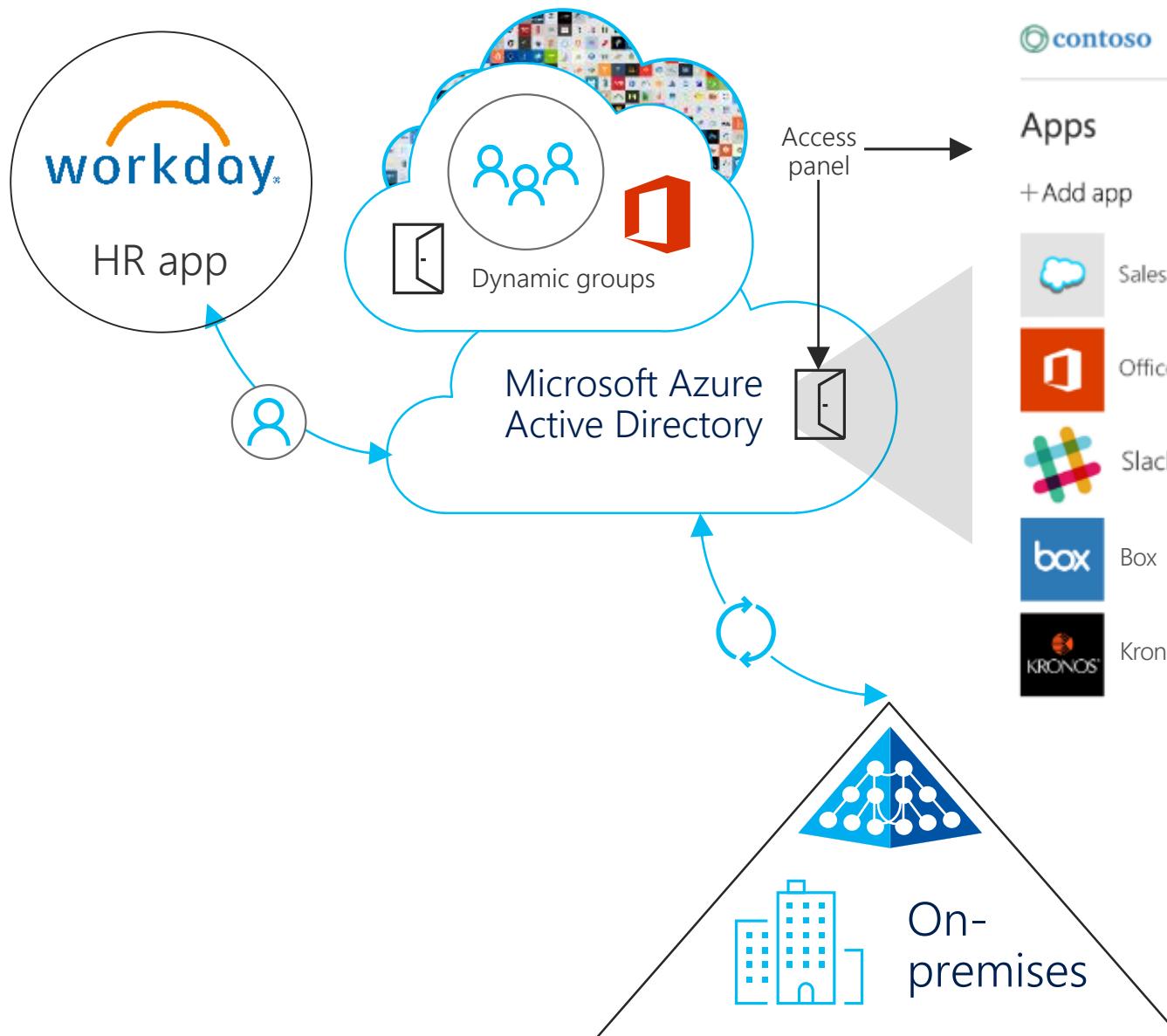
September 2018





MODERNIZE ACCESS

# Automated user lifecycle



contoso

Apps

+ Add app

| Icon       | App Name                        |
|------------|---------------------------------|
| Salesforce | ServiceNow                      |
| Office 365 | Workday                         |
| Slack      | Super Sensitive on-premises app |
| Box        | Office 365 SharePoint Online    |
| KRONOS     | Workplace by Facebook           |

Search apps

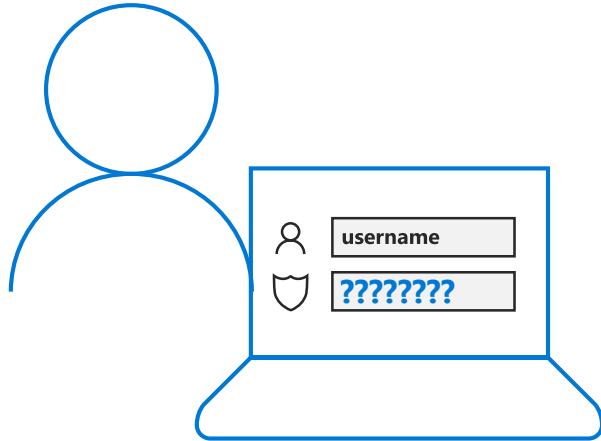
Groups

Access reviews



MODERNIZE ACCESS

# Empower user self-service to save time and money



- Resolving password issues for users is one of the largest IT costs
- Maximize user flexibility by enabling resets from an intuitive web interface or directly from the Windows login screen

The screenshot shows a 'change password' form on a 'contoso' website. At the top right, there's a navigation bar with three horizontal lines, a bell icon with a '5' notification, and a profile picture of a woman named Josilyn with the text 'CONTOSO CLOUD'. The main title is 'change password'. Below it, a note says: 'Strong password required. Enter 8-16 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.' The form fields are: 'User ID' (josilync@contoso.com), 'Old password' (empty input field), 'Create new password' (empty input field), 'Password strength' (empty input field), and 'Confirm new password' (empty input field). At the bottom are 'submit' and 'cancel' buttons.

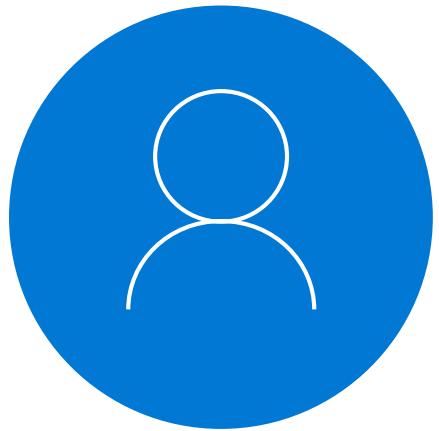
# Azure Active Directory

## Connect & Collaborate



CONNECT & COLLABORATE

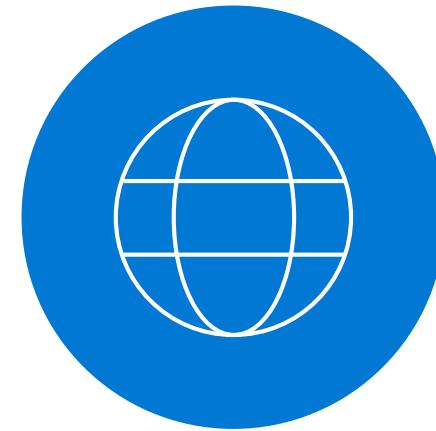
## Transform management of external identities



User-centric  
and flexible



Secure and  
reliable



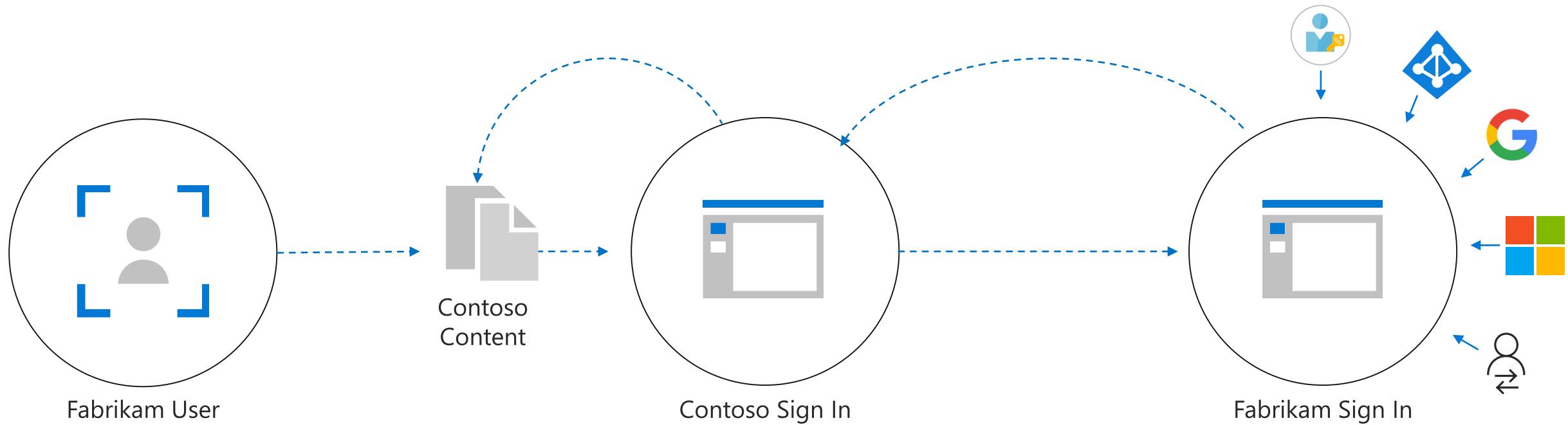
Global and  
scalable



CONNECT & COLLABORATE

# Seamless partner collaboration

Simplified collaboration with business partners around the world



Authentication separated from authorization

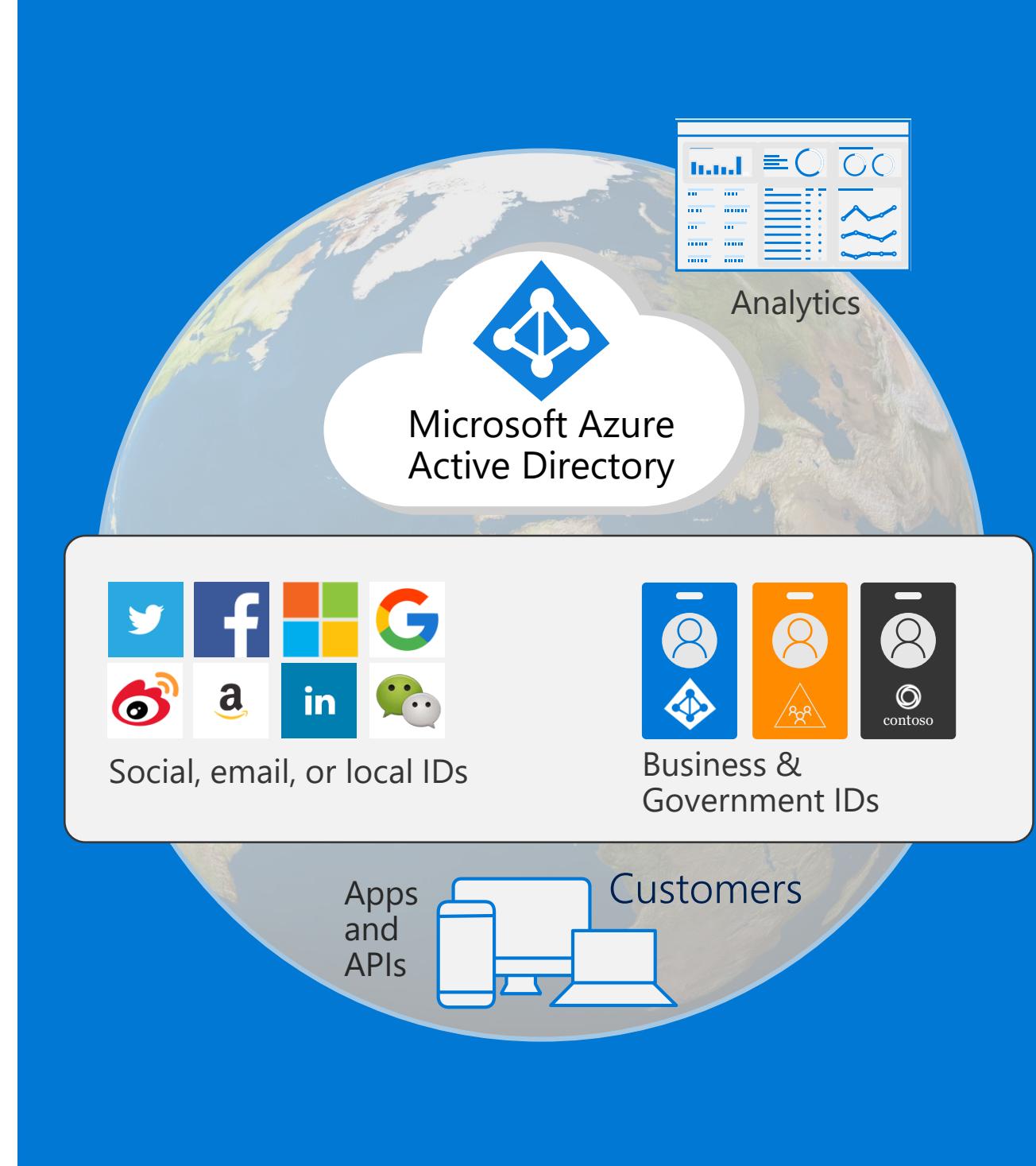


CONNECT & COLLABORATE

# Azure Active Directory B2C

Connect to any user on any platform

- ➔ Securely authenticate your customers using their preferred identity provider
- ➔ Capture login, preference, and conversion data for customers
- ➔ Provide branded (white-label) registration and login experiences





"Azure AD B2C was our solution of choice because it not only meets FERPA regulations, but it also helps us manage identities at scale, all while being cost-effective and secure."

Troy Neal  
Managing Director of Information Services



# Azure Active Directory

## Protect & Govern

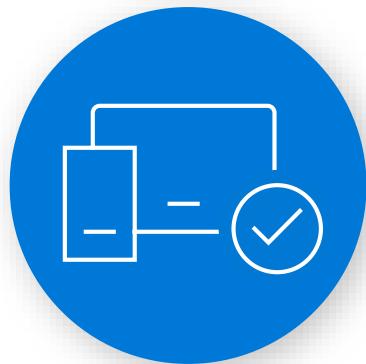


PROTECT & GOVERN

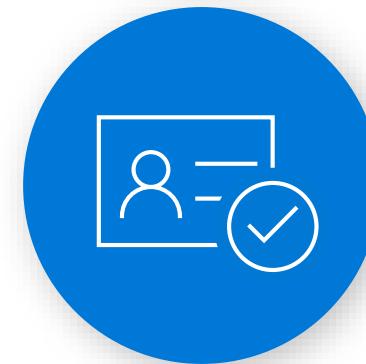
# Safeguard user credentials with a Zero Trust approach



Secure authentication



Conditional access



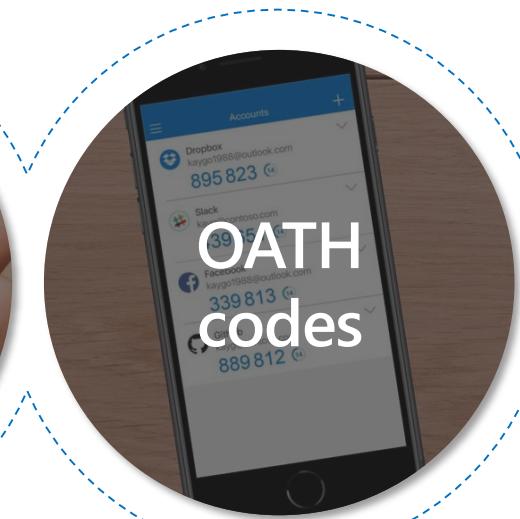
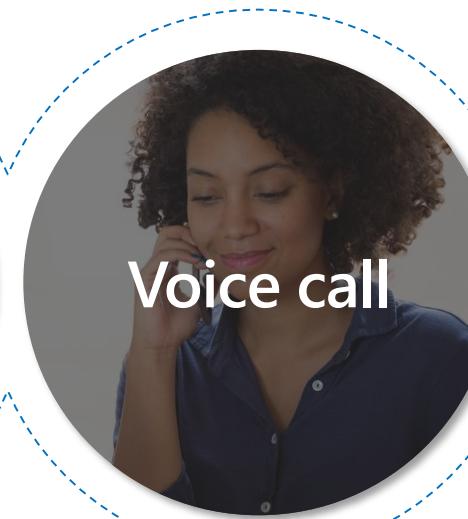
Identity protection

**Network walls have come down but your security doesn't have to.**



# Secure authentication using MFA

Multi-factor authentication prevents 99.9% of identity attacks

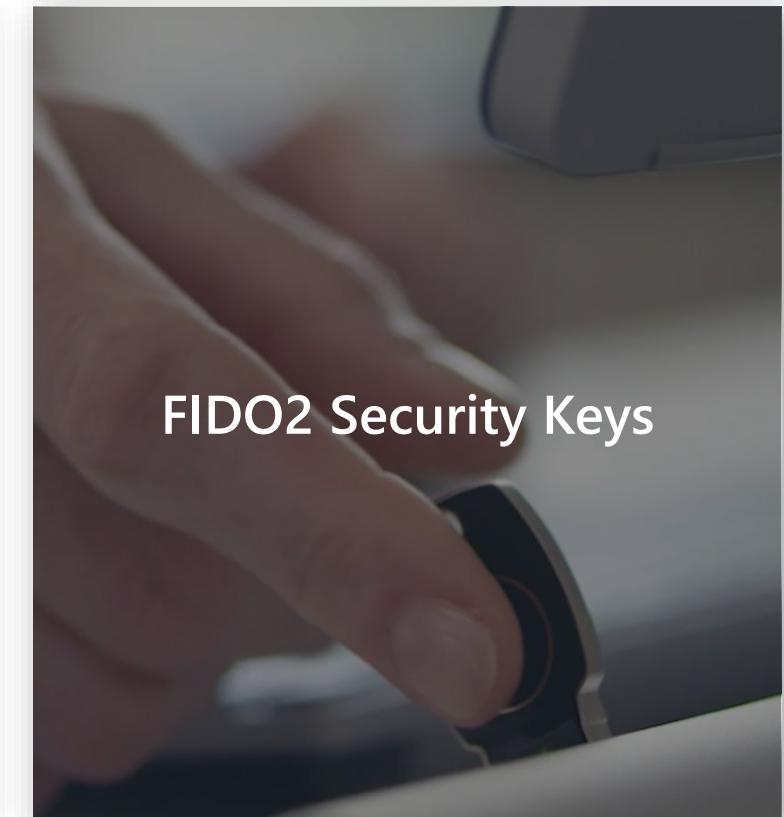
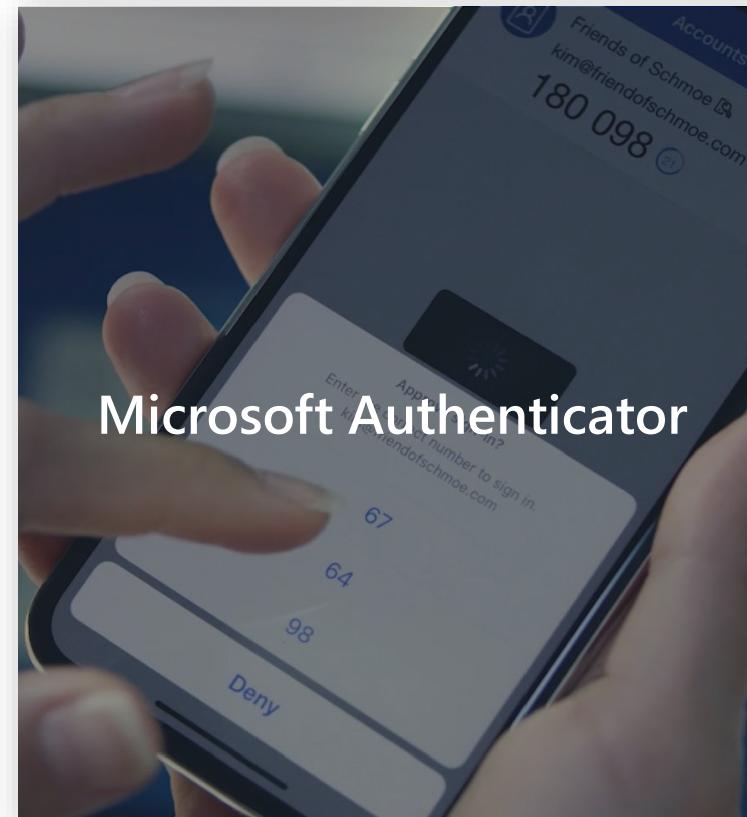
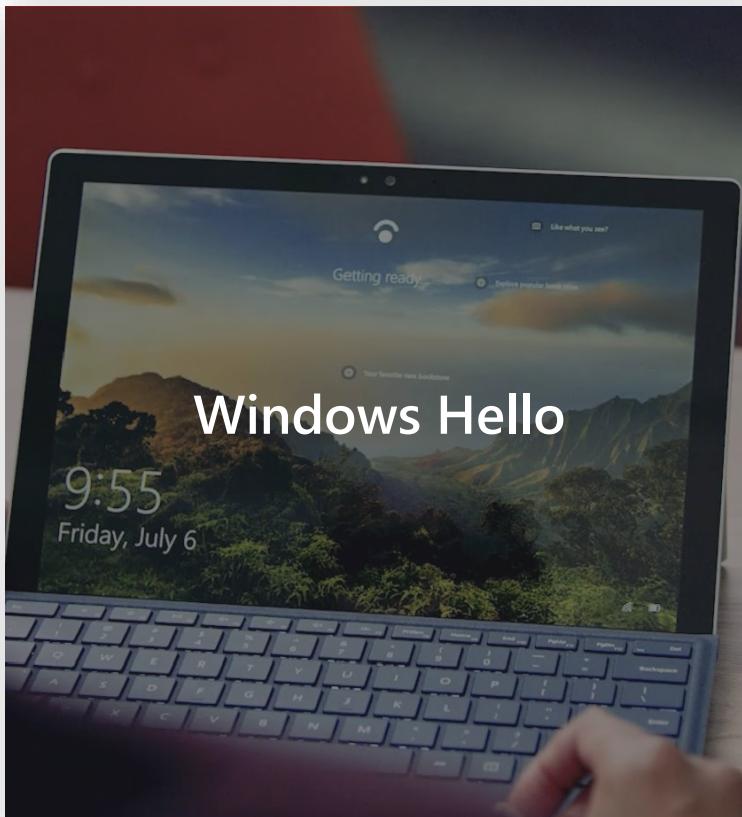




PROTECT & GOVERN

# Secure authentication with password-less credentials

High security convenient methods of authentication

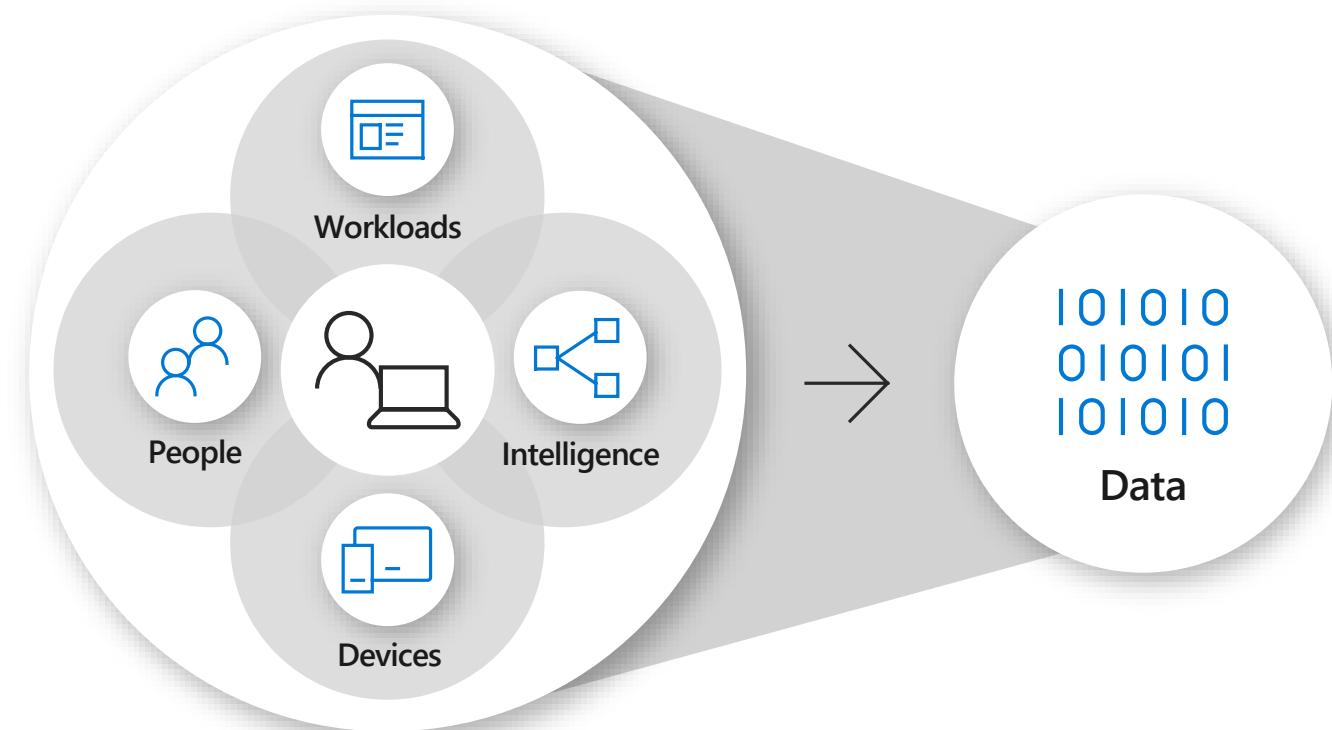
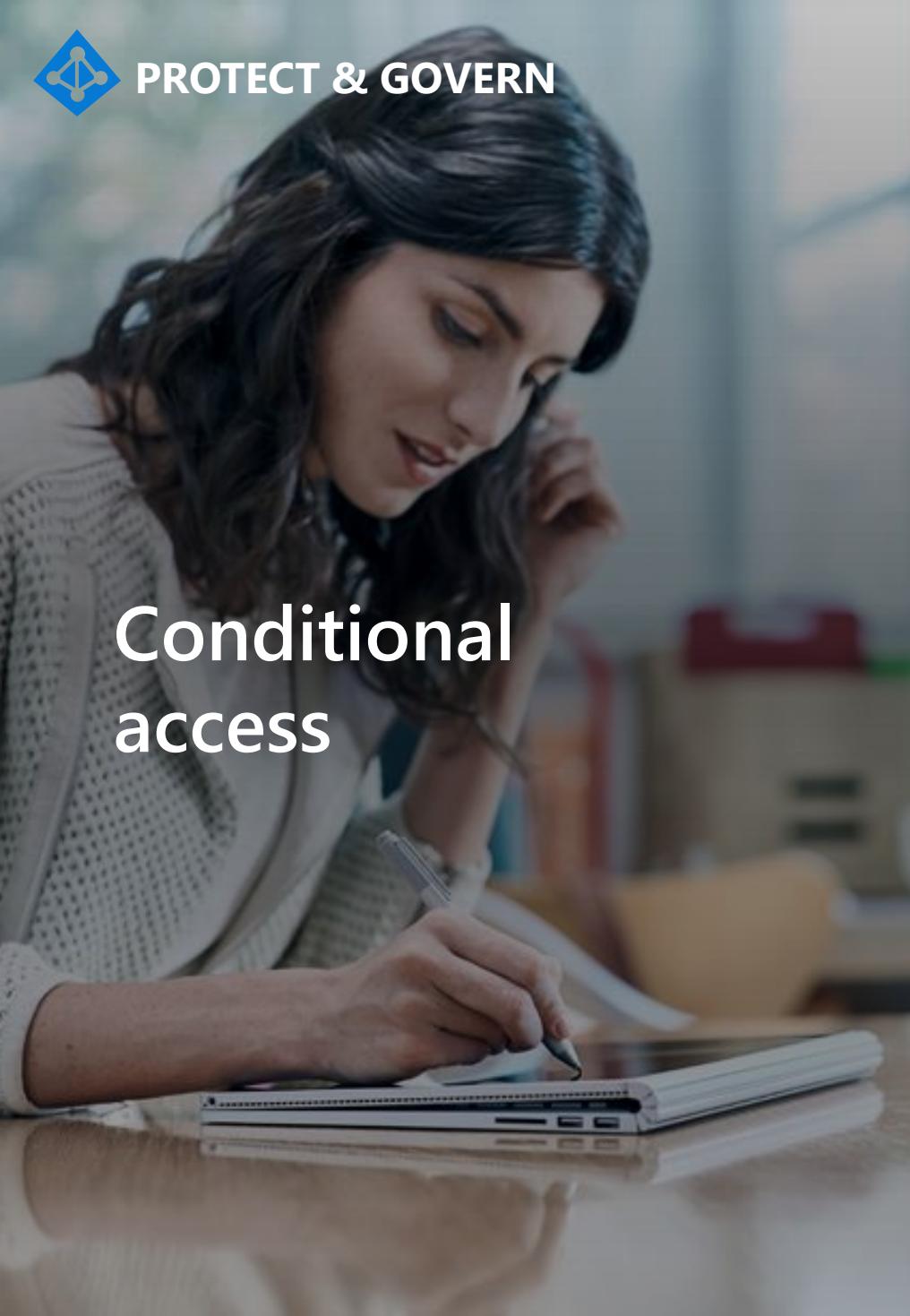


Get the whitepaper: [aka.ms/gopasswordless](http://aka.ms/gopasswordless)



PROTECT & GOVERN

## Conditional access



Implement Zero Trust with  
Azure AD conditional access

# Azure AD conditional access

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps

## Conditions

Employee & Partner  
Users and Roles



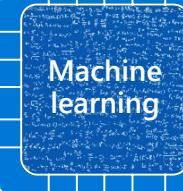
Trusted &  
Compliant Devices



Physical &  
Virtual Location



Client apps &  
Auth Method



Session Risk



Real time  
Evaluation  
Engine



Policies

Effective  
policy

## Controls

Allow/block  
access



Limited  
access



Require  
MFA



Force  
password  
reset



Block legacy  
authentication



Microsoft  
Cloud

Microsoft  
Cloud App Security



Cloud SaaS apps



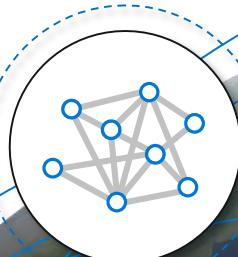
On-premises  
& web apps



# Azure AD Identity Protection

## Connected intelligence

Observe trillions of signals and risk events from cloud systems



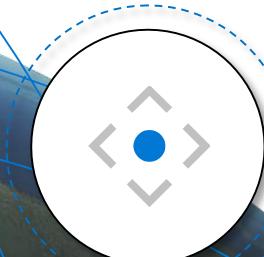
## Continuous detection

Apply artificial intelligence and human expertise to derive accurate insights



## Actionable insights

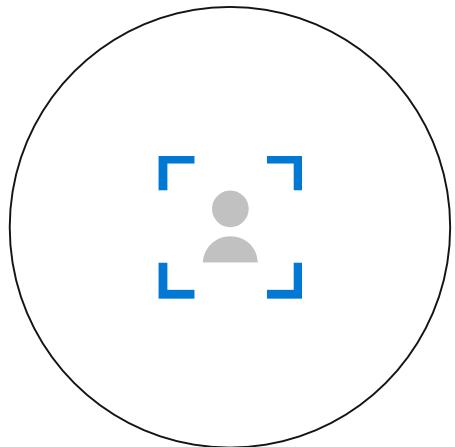
Send alerts, self-mitigate, and automatically remediate threats



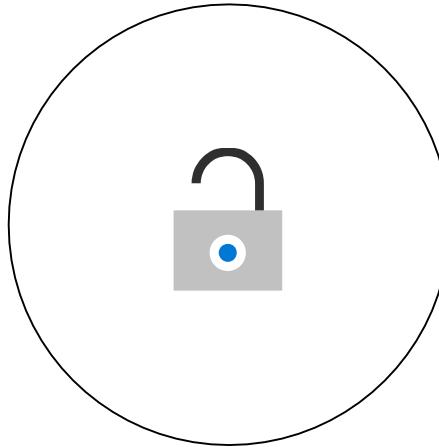


PROTECT & GOVERN

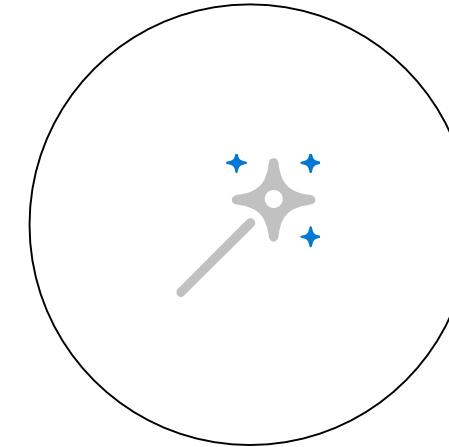
# Azure AD Identity Governance



**Identity lifecycle**  
facilitates collaboration



**Access lifecycle**  
provides seamless and  
efficient access



**Privileged access lifecycle**  
addresses risks inherent in  
administration

**Ensure the right users have the right access to the right resources**

# Azure Active Directory

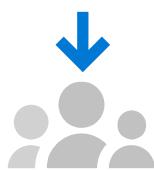
## Develop & Integrate



DEVELOP & INTEGRATE

# Microsoft identity platform for developers

Unified toolkit for building identity-connected applications



## Reach more users

Let your users sign in with their Microsoft personal or work account or using their social accounts



## Secure your application

Extend the security benefits and access controls to your customers who use Azure AD without additional code



## Create powerful apps

Build the next generation of apps and experiences by connecting to the Microsoft Graph



## Integrate with ease

Build with confidence with open industry standards on a trusted, reliable platform

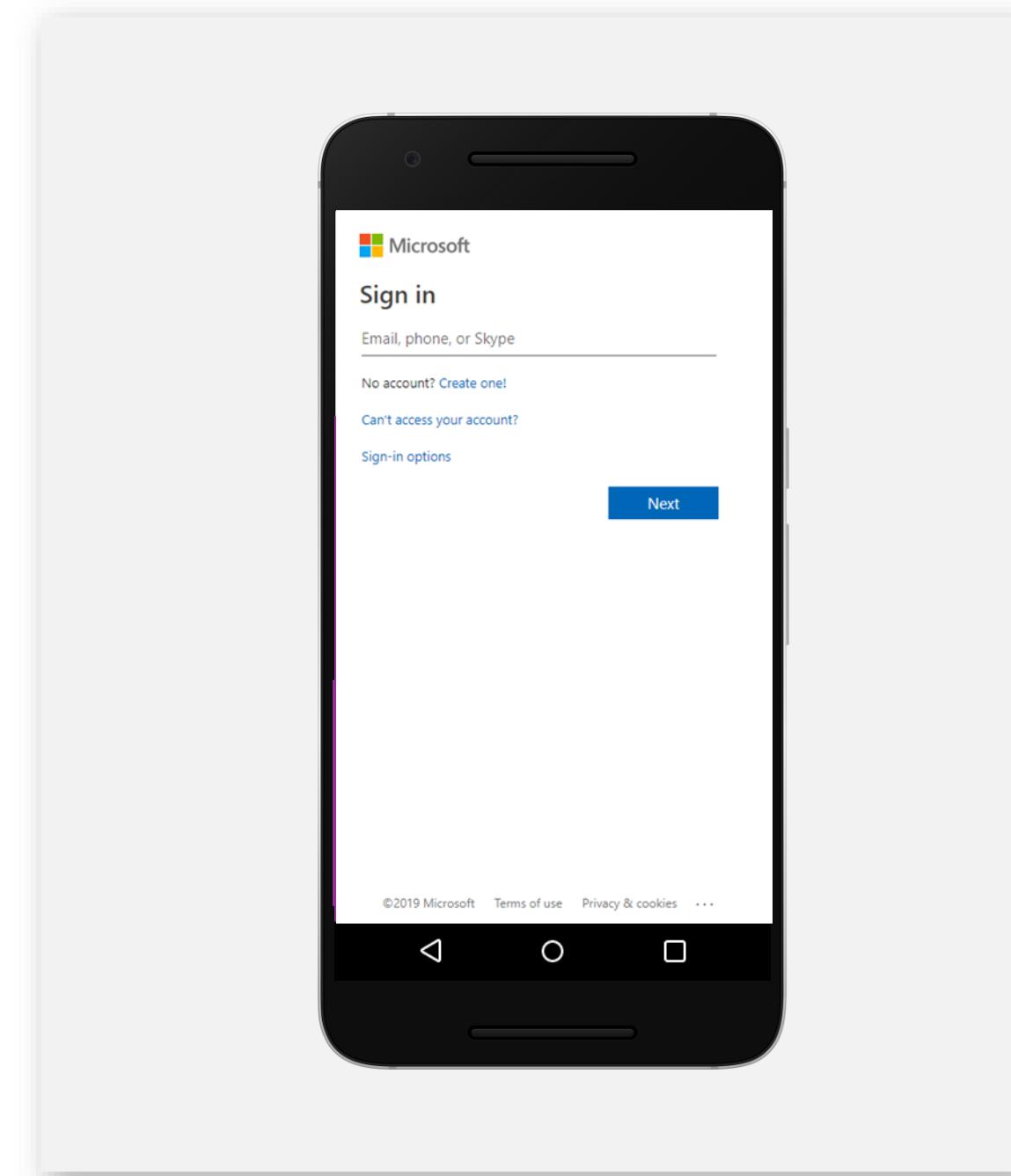


DEVELOP & INTEGRATE

# Add sign in with Microsoft

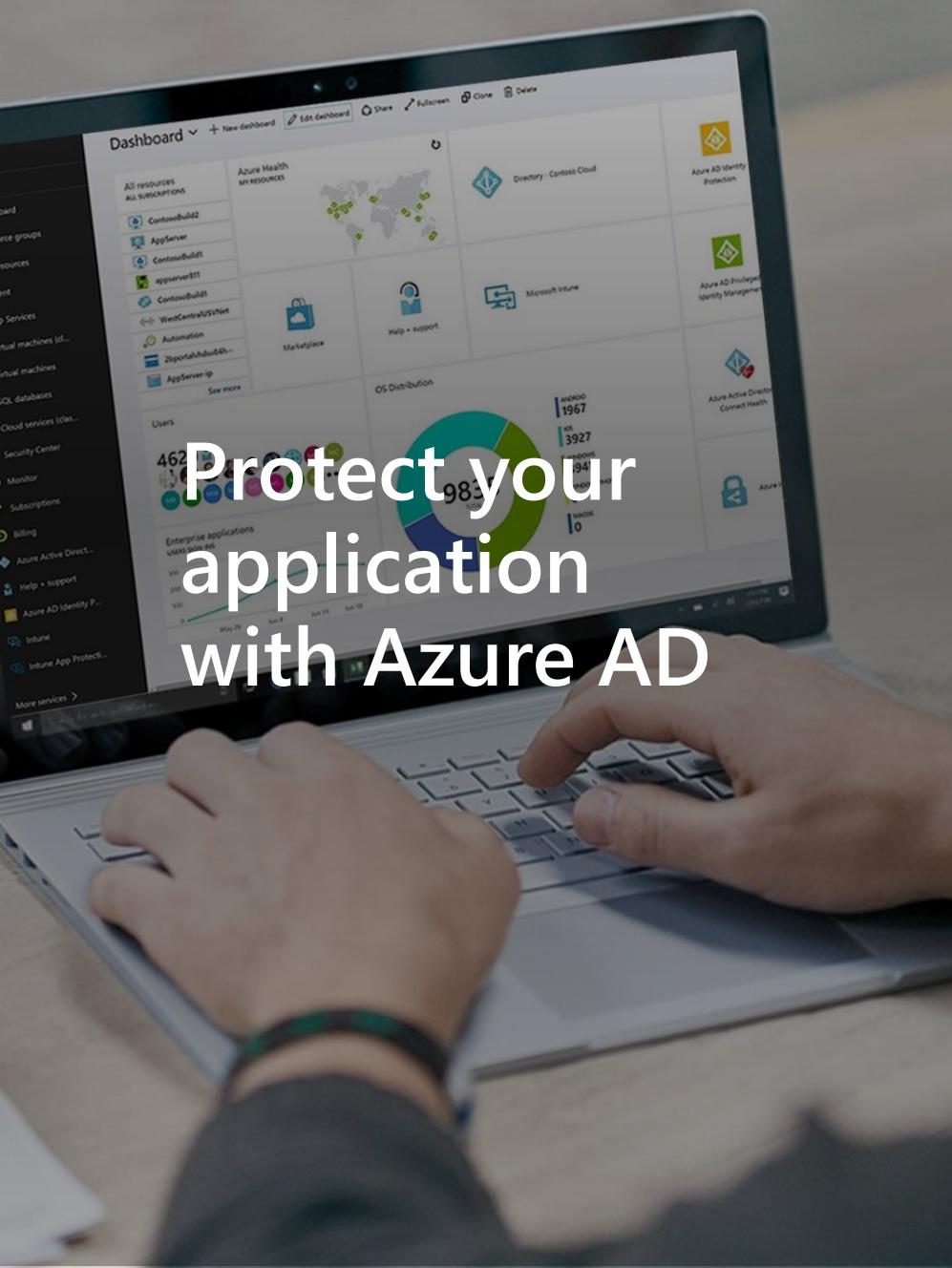
Reach a broad audience

- ➔ Sign in users with any Microsoft identity - Microsoft personal, work or school accounts
- ➔ One less username and password for your users to remember
- ➔ Reduce sign in friction and support costs





## DEVELOP & INTEGRATE



Protect your  
application  
with Azure AD

Give enterprises who use Azure AD as their identity and access management system the security benefits and access controls they know and trust.

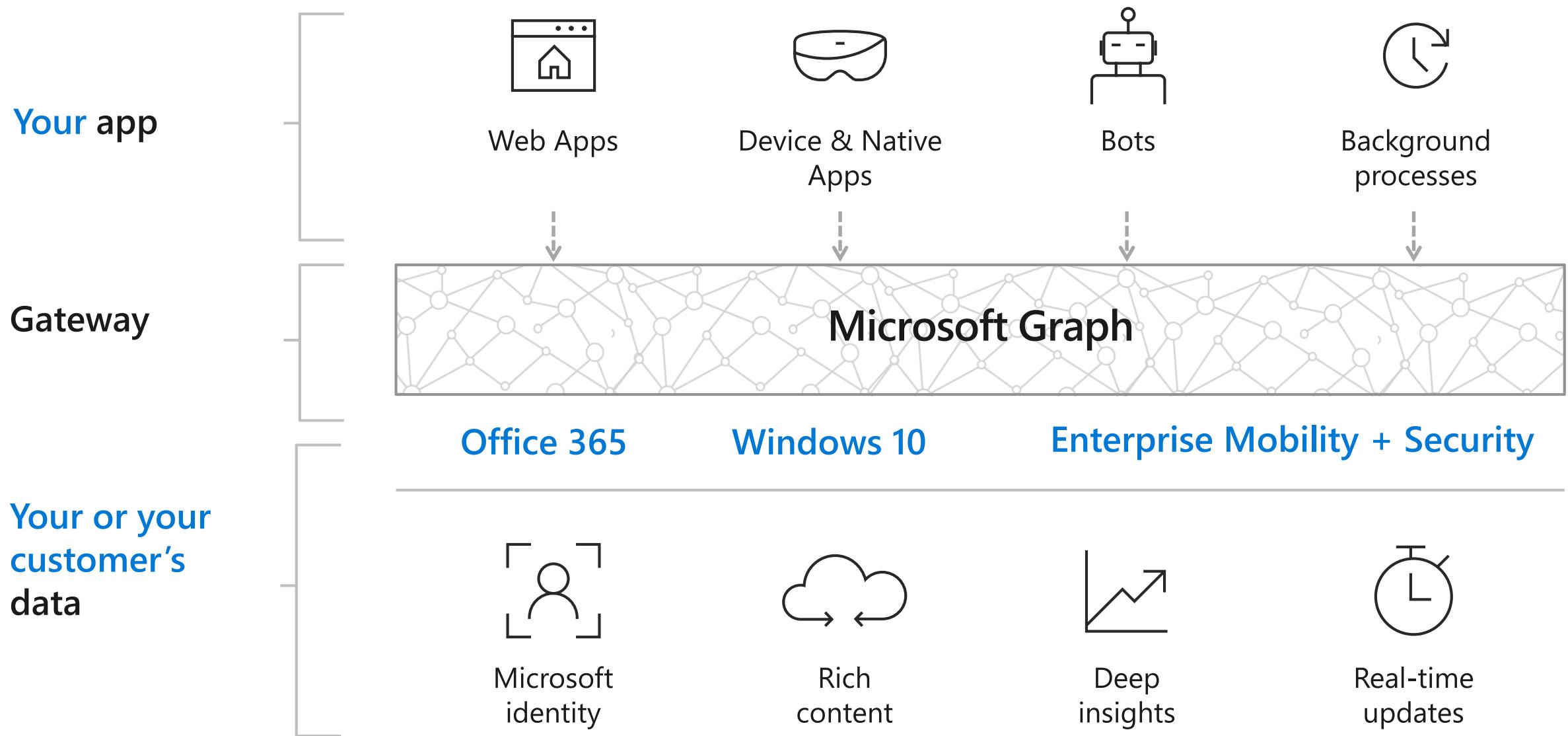
Secure access to users and their data in Microsoft APIs or your own APIs.

Build secure solutions with Microsoft Authentication Libraries available in multiple languages



DEVELOP & INTEGRATE

# Build smarter apps by connecting to Microsoft Graph





DEVELOP & INTEGRATE

# Integration Scenarios

How partners are integrating with Azure Active Directory



## Single sign on

Let your end users easily sign in with their Microsoft identity



## User provisioning

Automatically provision or de-provision your application to users



## Microsoft Graph

Connect to the data in the Microsoft Graph and build smarter applications

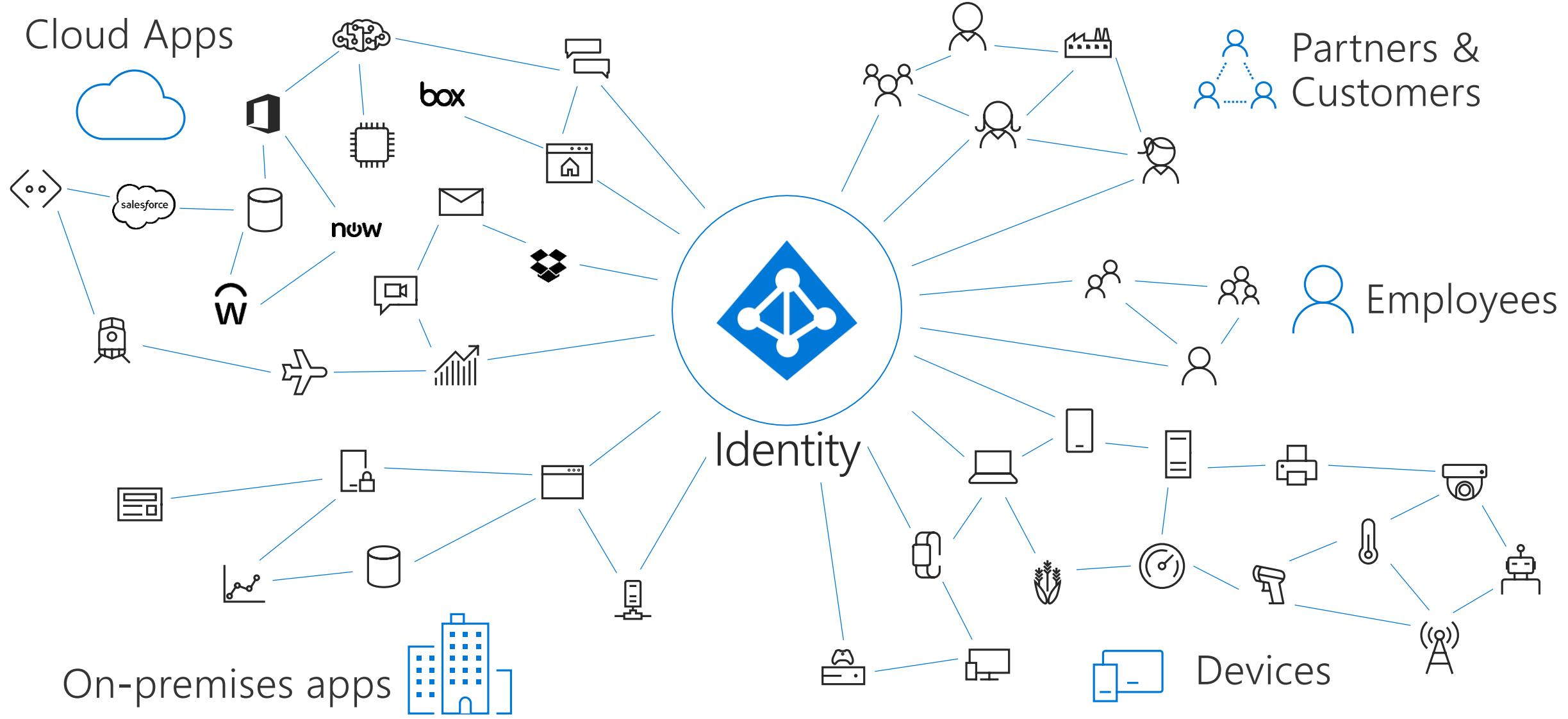


## Secure your cloud infrastructure (IaaS) with Azure AD

- Reduce vulnerability to credential attacks with multi-factor authentication and conditional access.
- Minimize access with Azure role-based access control and Privileged Identity Management.
- Stop managing local accounts for Virtual Machines with Azure AD sign in for Azure VMs
- Remove credentials from your code with managed identities for Azure resources.



# Identity is the new control plane

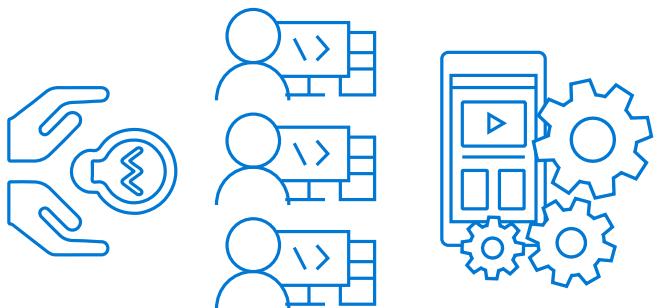


# Next steps

You may already be using Azure AD!



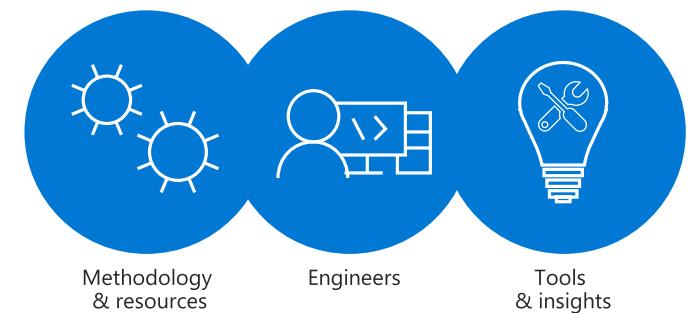
Try Azure Active Directory  
today for free



Let our team help with  
your implementation

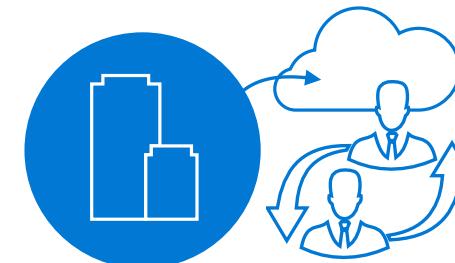
## Fast track

Expert partners and Microsoft Engineering  
remote assistance to accelerate your  
Azure AD deployment



## Get to production team

Microsoft Engineers engage directly to get you  
up and running with Azure Active Directory



## To Do List

1. Enable Azure Active Directory Premium
2. Enable Multi-Factor Authentication (MFA)
3. Enable Self-service Password Reset (SSPR) with Password Protection
4. Develop a plan to move your apps to Azure AD





# Thank you

# Five Steps to Protect Against Threats with Azure AD



## Strengthen your credentials

*MFA reduces compromise by 99.99%*



## Increase your awareness with auditing and monitor security alerts

*Attackers escape detection inside a victim's network for a median of 101 days. (Source: [FireEye](#))*



## Reduce your attack surface

*Blocking legacy authentication reduces compromise by 66%.*



## Enable self-help for more predictable and complete end user security



## Automate threat response

*Implementing risk policies reduces compromise by 96%*

*60% of enterprises experienced social engineering attacks in 2016. (Source: [Agari](#))*